Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

VERIZON COMMENTS ON FURTHER NOTICE

The Commission's declaratory orders authorizing more extensive robocall blocking are important and laudable steps forward in the war on robocalls.[1] The *Further Notice* correctly contemplates that the Commission and industry should take additional action to more aggressively prosecute that war.

First, if all voice providers do not voluntarily implement the STIR/SHAKEN call authentication technology, the Commission should ultimately require it. Otherwise illegal robocallers will have an avenue to continue to spam consumers across the United States by sending their calls through providers that choose not to participate. STIR/SHAKEN should also apply to calls originating from Voice over Internet Protocol (VoIP) providers located outside the United States. And the Commission should require any provider that has not yet implemented STIR/SHAKEN to confirm it has safeguards in place to avoid becoming a conduit that illegal robocallers can use to bypass the authentication framework. To manage and enforce this new

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59, FCC 17-151 (rel. Nov. 17, 2017); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, CG Docket No. 17-59, WC Docket No. 17-97 (rel. June 7, 2019) ("*Further Notice*").

framework, the Commission should establish a publicly-available registry where every provider must certify its compliance with the Commission's robocall rules.

The Commission also should promote increasingly robust call blocking by making clear that service providers do not face liability for blocking errors if they rely on reasonable analytics that include authenticating whether incoming calls pass validation under STIR/SHAKEN. And the Commission should continue to partner with industry to engage state and local government and other critical callers to develop databases and processes to ensure that their calls are not inadvertently blocked. These actions will support more aggressive and more effective blocking by service providers.

I. THE COMMISSION SHOULD ESTABLISH A COMPREHENSIVE CALL AUTHENTICATION FRAMEWORK.

Unless voluntary efforts quickly succeed, STIR/SHAKEN requires appropriate regulation. Otherwise, a handful of holdout carriers who fail to implement it will undercut its usefulness for consumers and participating service providers. While Verizon is committed to implementing STIR/SHAKEN, it can only validate the Caller ID of an incoming call for its customer if the provider that originated the call has also implemented STIR/SHAKEN. Without a trustworthy cryptographic "signature" from the originating provider vouching for the accuracy of the calling party number transmitted with each call, neither Verizon nor any other carrier can validate the Caller ID of calls to our customers. If a subset of providers do not "sign" their calls with STIR/SHAKEN, illegal robocallers will use those providers to send unsigned traffic to U.S. consumers—and those consumers will be harmed because that illegal unsigned traffic will comingle with legitimate unsigned traffic (e.g., from non-IP providers) and become impossible to separate.

A. STIR/SHAKEN Must Be Implemented Broadly, Including by Foreign VoIP Providers That Originate Calls to U.S. Consumers From U.S. Numbers.

As a starting point, the STIR/SHAKEN requirement should include all voice service providers that directly or indirectly send voice traffic to U.S. consumers using the called party's ten-digit telephone number, regardless of whether they are classified as interconnected or non-interconnected VoIP, or whether they provide one-way or two-way service. The regulatory framework should include appropriate exemptions (or extensions from the implementation deadline) for service providers that use Time Division Multiplexing (TDM) technology or that otherwise have traffic for which industry-standard techniques for signing calls with STIR/SHAKEN do not exist.[2] But the Commission should not exempt any IP-based provider based simply on its size. The results of industry tracebacks of illegal traffic indicate that the majority of illegal traffic originates not from large providers but rather from smaller IP-based ones. So while exemptions for smaller rural carriers may be appropriate, an across-the-board exemption based on a provider's size would create a huge gap in STIR/SHAKEN that invites certain providers to continue to originate spam robocalls to U.S. consumers.

The STIR/SHAKEN framework must protect U.S. consumers where U.S.-based service providers turn a blind eye to foreign providers sending calls to U.S. consumers from U.S. numbers. Industry tracebacks of illegal robocalls frequently dead-end when they reach a U.S.-based service provider that is accepting illegal traffic from a foreign IP-based provider because it is virtually impossible to shut down or punish either provider. It is therefore important to require STIR/SHAKEN for any provider, regardless of its geographic location, if it intends to permit its customers to make calls using U.S. telephone numbers. The rules also should prohibit any U.S.-

[2] *See* Section I-D, *infra*.

based service provider from accepting any voice traffic from any other provider if that provider has failed to certify to the Commission that it complies with the STIR/SHAKEN rule.

The STIR/SHAKEN rules need not apply to calls from providers subject to the jurisdiction of foreign regulators if those providers do not permit their callers to insert numbers from the U.S. portion of the North American Numbering Plan and send those calls to U.S. consumers. U.S.-inbound international calls originating from foreign telecommunications carriers with numbers corresponding to their countries' numbering plans do not currently materially contribute to the robocall problem and therefore do not need to be subject to the Commission's mandate.[3] The Commission should promote efforts by other countries to implement STIR/SHAKEN, and should support integrating those countries' STIR/SHAKEN regimes into the one being established here.

B. Providers With Traffic That Is Not STIR/SHAKEN-Enabled Should Certify That They Have Procedures to Avoid Originating Illegal Robocalls.

Because illegal robocallers can use calls not signed with STIR/SHAKEN to spam U.S. consumers, the Commission should require any provider that is permitted to originate traffic without signing it with STIR/SHAKEN to certify to the Commission that it takes appropriate measures to ensure that it is not contributing to the robocall problem. As Verizon has explained, there are various ways a service provider can avoid becoming part of illegal robocallers' attack vector, so the Commission should be non-prescriptive about how a service provider avoids

[3] In recent months, U.S. consumers have been increasingly harassed by the "Wangiri" scam, where bad actors spam them with calls from international phone numbers and then earn money from revenue- sharing arrangements with the foreign carriers that receive call-backs from the United States. Our experience is that those calls are usually *not* originated by the foreign telecommunications carriers, but rather arrive from VoIP providers with relationships with U.S. carriers.

serving illegal robocallers.[4] Any provider certifying that its end users are contractually or technically unable to originate large volumes of calls, such as wireless providers, would comply with this requirement. Other providers may rely on some combination of requiring compliance with law provisions in their customer contracts, monitoring customers' traffic patterns, and cooperating with law enforcement agencies (pursuant to appropriate legal process) to assist in government investigations of any customers suspected of illegal activity.

The right check on whether a provider's robocall mitigation program is sufficient should be whether tracebacks of suspected traffic by law enforcement agencies or USTelecom frequently identify the service provider as likely looking the other way when receiving traffic it should know is illegal. No service provider can ensure that none of its customers will engage in illegal conduct, so the Commission should not assume that a provider's procedures are deficient if it is infrequently identified via tracebacks or enforcement investigations as the source of illegal traffic. Nor would it be appropriate for the Commission to expect any service provider to police its customer base and second-guess whether its enterprise customers are in compliance with all applicable laws such as the Telephone Consumer Protection Act—it would not be appropriate or scalable for providers to attempt to make such subjective judgments about their customers. So if an enterprise customer is sued for an alleged violation of the Telephone Consumer Protection Act, but is not spoofing unauthorized numbers to avoid detection and is not hiding from enforcement authorities, the Commission should not conclude that its originating service provider's procedures are inadequate.

---

[4] *See In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, Comments of Verizon on Public Notice, CG Docket No. 17-59, Section II-C (July 20, 2018).

Instead, for service providers that are consistently found to be the origination point of illegal robocalls, despite warnings that traffic coming from their networks is suspected to be illegal, the Commission should scrutinize their robocall mitigation practices and their customer relationships. The Commission's rules could include putting such a service provider on "probationary" status if it is found to be the source of suspected illegal traffic even after being informed that suspicious traffic was identified as coming from its network. For example, the Commission could require providers on probation to provide details about their robocall mitigation practices; to monitor their end users' traffic patterns; to report to the Commission on the identities, locations, and traffic patterns (including spoofing patterns, call durations, and un-answer rates) of their customers; and to describe the corrective action they have taken after being notified about customers' suspicious traffic. If the Commission finds that a substantial portion of a provider's traffic continues to be illegal after this probationary period, it should prohibit that provider from handling any voice traffic destined for U.S. consumers (as discussed in Section I.D below).

C. The Commission Should Establish Registration and Reporting Obligations to Create Transparency About Every Provider in the Call Path and to Enforce the STIR/SHAKEN Mandate.

To create transparency about what providers are sending calls to U.S. consumers and enforce the Commission's STIR/SHAKEN rules, the Commission could require every provider to register with the Commission before sending calls from U.S. numbers to U.S. consumers. Every registrant that is an originating provider (i.e., that initiates calls on behalf of end users) should be required to certify that its traffic is signed with STIR/SHAKEN, and for any unsigned traffic it should be required to certify that it follows reasonable robocall mitigation procedures (as discussed in Section I-B above). Every registrant that is a transit provider (i.e., that receives

traffic from other service providers and sends it to downstream providers) should be prohibited from accepting traffic from any unregistered wholesale customer, and should be required to report to the Commission the percentage of calls from each upstream provider that are signed with STIR/SHAKEN. The Commission can leverage such a registry both to monitor compliance with the STIR/SHAKEN rules and also to ensure that non-compliant providers' traffic is not accepted onto the U.S. network.

By prohibiting transit providers from accepting traffic from unregistered providers, the Commission can meaningfully enforce the STIR/SHAKEN mandate. If a provider is not complying with its obligation to either sign calls with STIR/SHAKEN or to follow appropriate robocall mitigation procedures, by terminating that provider's registration the Commission can prohibit downstream providers from receiving its traffic. To identify such non-compliant service providers, the Commission could rely on downstream transit providers' reporting of which carriers send unsigned traffic, and for traffic not sent with STIR/SHAKEN it could use the results of tracebacks of illegal robocalls to identify providers that have consistently failed to implement sufficient robocall mitigation techniques.

The Commission could establish such a registry by leveraging the work already done to establish the Rural Call Completion registry.[5] It should set up that registry before a STIR/SHAKEN mandate goes into effect so that terminating carriers can promptly begin using the registry to protect their customers prior to the official government mandate. Once the registry is populated, downstream providers looking to protect their customers will be able to contractually require that all providers sending calls to their customers be registered and be listed

[5] S*ee Rural Call Completion*, Third Report and Order, 33 FCC Rcd 8400, 8407, ¶ 17 (2018).

as having certified compliance with either the STIR/SHAKEN or the robocall mitigation requirements. Thus, even prior to industry-wide STIR/SHAKEN deployment becoming a reality, industry can use the registry to protect consumers.

D. The Commission Should Require Providers to Follow Industry Practices to Ensure That STIR/SHAKEN Signatures Correctly Attest to Accuracy of Calling Party Number Information.

For STIR/SHAKEN to benefit consumers by ensuring that they receive accurate Caller ID information, the Commission should require originating service providers to not merely sign the calls they originate, but to ensure that their signatures accurately attest that their customers are using authorized numbers. There is nothing about the STIR/SHAKEN technology that automatically ensures that Caller ID information can be validated. To the contrary, while STIR/SHAKEN is a tool that holds promise for benefitting consumers if used responsibly, if that tool is misused or sloppily used it may not achieve its potential and indeed could cause consumer harm by incorrectly validating numbers that are in fact improperly spoofed.

If a carrier is permitted to sign a call with STIR/SHAKEN without knowing that the calling party number transmitted with the call is in fact correct, then the signature is useless for validating the Caller ID of the incoming call. Indeed, if consumers receive incorrectly "verified" calls because originating providers sign improperly-spoofed calls, then STIR/SHAKEN may *harm* consumers by incorrectly indicating that the Caller ID of such calls can be trusted. It is thus important that the STIR/SHAKEN mandate include a requirement that originating carriers follow appropriate industry-developed procedures to ensure that when attesting to the accuracy of the calling party number, the number is in fact accurate. Any service provider found to consistently sign improperly-spoofed calls should be de-listed from the registry of providers authorized to send calls to U.S. consumers.

In promulgating the STIR/SHAKEN mandate, the Commission should recognize that ensuring meaningful STIR/SHAKEN attestations may delay full implementation of STIR/SHAKEN for some originating call use cases. While in some cases it is relatively simple to ensure the accuracy of the number a customer is using to make calls, in other situations it is complex. The simplest case is where an enterprise uses numbers associated with the service provider that exclusively carries the enterprise's outbound traffic and therefore can sign those calls with full knowledge that they are not improperly spoofed. That STIR/SHAKEN signing scenario is one where originating providers can readily comply with a requirement that their signatures be meaningful. But limiting signing to that specific scenario would limit customer choice by prohibiting other use cases that are more complex but that are not yet candidates for meaningful (i.e., trustworthy) STIR/SHAKEN signatures.

Those more challenging cases include enterprise outbound traffic using calling numbers from one service provider, but carried on one or more other service providers. In that scenario (which is common), each originating provider will need to employ techniques to confirm that the telephone numbers its customer is using are ones that it has either been assigned by another provider or authorized to use by another party. A special sub-scenario of these use cases involves calling numbers that are toll free numbers that may span multiple service providers. Other complex emerging scenarios—which raise both technical and policy issues—include enterprises or call centers that have an interest in and the capability to sign their calls independent of their service providers. Policies on whether the originating service provider must in all cases pass such signatures will drive architectural solutions. Voice providers implementing STIR/SHAKEN also need to address over-the-top applications where calling numbers may be used for outbound traffic that enters the Public Switched Telephone Network through one or

more service providers. For these and other complex use cases, industry is analyzing business requirements and developing mechanisms and practices that originating carriers can use to confirm that the numbers they are attesting to are accurate.[6] While those practices are under development, the Commission should require any provider originating unsigned traffic to certify in the interim that it follows appropriate robocall mitigation procedures.

Some industry observers incorrectly argue that even STIR/SHAKEN attestations that do not attest to the accuracy of the calling party number sent with the call are potentially useful and therefore industry should be permitted or encouraged to sign calls for customers even if they may be improperly spoofed. The STIR/SHAKEN standard includes the option for providers to insert "B" level attestations (if they know who made the call but do not know whether the calling party number is accurate) or "C" attestations (if the call comes arrives unsigned from another provider, so the provider supplying the attestation does not know the identity of the caller).[7] The argument in favor of permitting these lower-level attestations focuses on the fact that such signatures can be useful for efficiently tracing back a suspicious call to the source. But that rationale for permitting these lower-level attestations would leave gaps. First, industry traceback techniques

---

[6] *See, e.g.*, ATIS/SIP Forum IP-NNI Task Force, ATIS Technical Report on a Framework for SHAKEN Attestation and Origination Identifier (2019), https://access.atis.org/apps/group_public/download.php/47803/IPNNI-2019-00003R005.docx; ATIS/SIP Forum IP-NNI Task Force, SHAKEN data exchange between service providers and enterprises (2018), https://access.atis.org/apps/group_public/download.php/42047/IPNNI-2018-00065R001.docx; ATIS/SIP Forum IP-NNI Task Force, Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Delegate Certificates (2019), https://access.atis.org/apps/group_public/download.php/47129/IPNNI-2019-00021R001.docx; ATIS/SIP Forum IP-NNI Task Force, Best Current Practices on the protection of STIR/SHAKEN data between service providers and from service providers to enterprises (2019), https://access.atis.org/apps/group_public/download.php/47467/IPNNI-2019-00055R000.docx; ATIS/SIP Forum IP-NNI Task Force, ATIS Technical Report on a Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements (2019), https://access.atis.org/apps/group_public/download.php/48148/IPNNI-2019-00071R002.docx.

[7] *See* ATIS/SIP Forum IP-NNI Task Force, Errata on ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN) (2019), https://access.atis.org/apps/group_public/download.php/46536/ATIS-1000074-E.zip.

can now efficiently identify the source, so there is no need to use STIR/SHAKEN as a crutch for that purpose. More importantly, permitting service providers to default to these lower-level STIR/SHAKEN attestations would mean that calls from these service providers—even though they have put STIR/SHAKEN into their networks—cannot be validated on behalf of consumers, which in turn would compromise STIR/SHAKEN's mission of restoring trust in Caller ID. Accordingly, any benefits of permitting "B" or "C" attestations are outweighed by the benefits of driving the industry towards signing calls with more trustworthy (i.e., "A" level) attestations.

E. The Commission Should Require Transit Providers to Pass STIR/SHAKEN Signatures Unaltered.

A service provider terminating a call to its customer can only validate the associated calling party number if it arrives with a valid STIR/SHAKEN token, i.e., the cryptographic signature under the STIR/SHAKEN protocol that the originating provider inserts in one of the headers that is transmitted with IP calls. That token must arrive intact after the call passes from the originating provider (which signed the call) and through transit providers (in the middle of the call path) that ensure the token is not stripped or modified during the call path. The Commission should therefore require transit carriers receiving IP traffic over IP interconnections to pass the STIR/SHAKEN information unaltered so that the carrier terminating the traffic to its end users can use the tokens to validate the Caller ID for incoming calls.

II. THE COMMISSION SHOULD ESTABLISH A SAFE HARBOR FOR SERVICE PROVIDERS THAT BLOCK CALLS USING REASONABLE ANALYTICS THAT INGEST THE STIR/SHAKEN VERSTAT.

As long as a provider uses reasonable analytics to identify unwanted robocalls, and that program includes ingesting the STIR/SHAKEN verification (the "verstat" in the standards bodies' nomenclature), the service provider should not be liable for erroneously blocked calls. Such a policy will support the goal of incentivizing service providers to protect consumers with

increasingly robust blocking solutions. Errors do occur, albeit infrequently, with even the most sophisticated call blocking analytics, but the consumer benefits of blocking outweigh the potential downside of a small number of errors. Therefore, consumers will benefit from a strong safe harbor giving providers a green light to block more aggressively.

III. THE COMMISSION SHOULD WORK WITH INDUSTRY TO DEVELOP A FRAMEWORK FOR ENSURING CRITICAL CALLS ARE NOT BLOCKED.

The Commission correctly emphasizes that blocking must include processes and procedures to avoid blocking critical calls, such as from state and local public safety agencies. Verizon and other providers of blocking services already take steps to avoid inadvertently blocking such calls. But the industry and legitimate government callers would benefit from standardization, including the development and maintenance by those agencies of a single authoritative list of critical call numbers on which service providers can rely.

The Commission and industry also should partner both to develop the right framework for avoiding the blocking of critical calls and to educate Public Safety Answering Points (PSAPs) and other critical calling stakeholders about how call blocking works and how they can ensure their calls are not blocked. For example, there is anecdotal evidence that some public safety entities have historically used invalid numbers for certain purposes. In those cases it is important to make those stakeholders aware that the blocking the Commission authorized with its November 2017 declaratory order potentially could block those sorts of calls.

Finally, the Commission and industry should work together to address the risk that bad actors will increasingly spoof critical numbers. As call blocking tools become more widespread and more effective, illegal robocalls whose contact rates are falling may well begin to impersonate critical calling entities in order to ensure that their calls are not blocked. Tracing back and prosecuting actors that engage in such malicious spoofing should be a high priority, and

Verizon stands ready with other members of the USTelecom Traceback Group to prioritize tracebacks of any such calls.

CONCLUSION

The Commission should seize the opportunity to take the fight to illegal robocallers by ensuring widespread implementation of STIR/SHAKEN in ways that will maximize its benefits to consumers, including by requiring any provider that does not sign its calls to certify that it has appropriate practices to avoid originating illegal traffic. It should also help industry more effectively block unwanted robocalls by granting an appropriate safe harbor for erroneous blocks and by helping developing a framework to avoid blocking calls from public safety and other critical entities.

Respectfully submitted,

/s/ Christopher D Oatway

William H. Johnson
Of Counsel

Gregory M. Romano
Christopher D. Oatway
1300 I Street, N.W.
Suite 500 East
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon

July 24, 2019